

**UNITED STATES DISTRICT COURT  
DISTRICT OF NEW MEXICO**

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No. 17-CR-3402MV

CHRIS BANDY,

Defendant.

**MEMORANDUM OPINION AND ORDER**

**THIS MATTER** is before the Court on Defendant Chris Bandy's Motion to Suppress Evidence. Doc. 53. The Government filed a response in opposition [Doc. 54] and Mr. Bandy did not file a reply. The Court, having considered the motions, relevant law, and being otherwise fully informed, finds that Mr. Bandy's Motion to Suppress Evidence is not well-taken and will be **DENIED**.

**BACKGROUND**

Mr. Bandy is charged in a one-count indictment with Stalking in violation of 18 U.S.C. § 2261(A)(2)(B). Doc. 2. The charge arises from his alleged use of interactive and electronic computer services to cause substantial emotional distress to his victim, M.D., from December 2016 through January 2017. Doc. 54 at 3–5.

**I. Factual Background**

The Government alleges that Mr. Bandy was employed at Nusenda Credit Union (Nusenda) as an information technology (IT) specialist from July 2006 to February 2014, but that he was fired after numerous incidents in which he was belligerent, yelling at his manager, making accusations, and using unprofessional language. Doc. 54 at 1. The victim of Mr. Bandy's alleged stalking, M.D., was the Senior Vice President of Human Resources who oversaw Mr. Bandy's

termination. *Id.* at 1–2. Following his termination, the Government alleges that Mr. Bandy sent M.D. an email on December 9, 2016 from a disguised email address with the subject line “Job Interview” and a message describing graphic sexual content attributed to her, such as pole dancing and prostitution. *Id.* at 2. The Government used metadata from the email to establish that it originated from Mr. Bandy’s Internet Protocol (IP) address, 71.228.120.233. *Id.* The email was also recovered from Mr. Bandy’s laptop after the Federal Bureau of Investigations (FBI) searched his residence in February 2017. *Id.*

After one of Mr. Bandy’s former managers was fired from Nusenda in 2016, Mr. Bandy allegedly used that manager’s identity to send more abusive emails: on December 14, 2016, he sent an email to M.D. and other employees at Nusenda that was sexually graphic and degrading. *Id.* at 3. This email was also traceable to Mr. Bandy’s laptop. *Id.* A third email was sent on December 31, 2016, a fourth email on January 11, 2017, and a fifth email on January 27, 2017, each with similar sexually graphic subject matter. *Id.* at 3–5. The fifth email was also recovered from Mr. Bandy’s laptop after the Federal Bureau of Investigations (FBI) searched his residence in February 2017. *Id.* at 5. Many of the emails referenced the author watching M.D. at home and in the office, with a particular emphasis on observing her in the bathroom and in the shower. *Id.* In addition to the emails, the Government alleges that Mr. Bandy targeted M.D. with Tweets from multiple Twitter accounts. Doc. 54 at 5. The Twitter messages had similar content as the emails, referencing sexual matters and someone watching M.D., and each one “mentioned” her Twitter account using the “@” symbol so that the Tweets would appear in her notifications and on the newsfeeds of those that followed her account. *Id.*

After M.D. began receiving increasingly obscene emails in December 2016, the FBI special agents assigned to this case used the metadata from the emails to determine that the emails

originated from IP address 71.228.120.223 corresponding to the Albuquerque area. Doc. 54 at 10. Comcast owned this IP address, and a grand jury issued a subpoena to the Comcast Legal Response Center on January 13, 2017. *Id.* at 10–11. The subpoena requested (1) the subscriber information for IP address 71.228.120.223 on December 9th, 2016, including the subscriber’s name and other identifying information, and (2) subscriber information for Mr. Bandy, including identifying information and dates of service. *Id.* Comcast returned the subpoena and identified IP address 71.228.120.223 as being assigned to Mr. Bandy on December 9, 2016. *Id.* The IP address was assigned at Mr. Bandy’s address and the account contained the username *BaiMeiHan*. *Id.* at 11.

In addition to the Comcast subpoena, the Government served a search warrant on Twitter. *Id.* at 5. Information from these investigations established that Mr. Bandy’s subscriber account was assigned to an IP address that logged into Nusenda’s internet banking system and sent the emails from his residence with a user ID for the account of *BaiMeiHan*. *Id.* at 5–6. Twitter records also established that the same IP address registered to Mr. Bandy was used to create the account that posted the messages at issue. *Id.* at 6. Next, the Government applied for a search warrant to search Mr. Bandy’s residence and electronic computer devices. Doc. 54 at 12. The affidavit that accompanied the application “enjoyed a breadth considerably more extensive than just the information” from the Comcast subpoena. *Id.* The affidavit included information from multiple witness interviews and “numerous subpoenas issued and the information processed from their returns.” *Id.* The affidavit described how FBI special agents confirmed that Mr. Bandy’s address belonged to him by searching the Bernalillo County Assessor’s Office, cross-checking with former employers, surveilling the property, and observing him and his vehicle at the residence. *Id.*

The affidavit also detailed how the degrading and obscene emails sent to M.D. were traced back to Mr. Bandy: After determining that IP address 71.228.120.223 was linked to the emails,

Nusenda searched their internet banking system to determine whether anyone had previously connected to their systems with that IP address. Doc. 54 at 13. Their search indicated that user Chris Bandy, with the username *BaiMeiHan*, had logged into his personal banking account with this IP address on three occasions between November 1, 2016 and January 13, 2017. *Id.* The IP address 71.228.120.223 had been registered to Mr. Bandy both before *and* after the harassing emails were sent. *Id.* The search warrant was executed on Mr. Bandy's residence on February 3, 2017, and a laptop computer was recovered. *Id.* The laptop contained the emails from December 9 and 14, 2016, as well as January 27, 2017. *Id.*

## **II. Procedural Background**

The grand jury returned an indictment on December 5, 2017 charging that Mr. Bandy used electronic communications to harass and intimidate in a manner that would reasonably be expected to cause emotional distress. Doc. 2; Doc. 54 at 7. Mr. Bandy was arrested on December 7, 2017, and he pled not guilty to the charge at an arraignment held the same day. Doc. 54 at 7; Doc. 5. He was released on conditions, but on June 5, 2018, the probation office filed a petition for actions on Mr. Bandy's conditions of release for contacting the husband of the victim, M.D., at an auto care business bearing her surname. *Id.* Mr. Bandy absconded from his halfway house on July 3, 2018 and was arrested in Southern Texas on August 4, 2018. *Id.* at 7–8. Mr. Bandy began filing motions *pro se* while in custody in Texas, and after he was returned to New Mexico the Court held a *Faretta* hearing to determine his ability to proceed *pro se*. Doc. 99. On October 21, 2020, the Court granted Mr. Bandy's Motion for Self-Representation and the Appointment of Stand-By Counsel [Doc. 73], with attorney Nicholas Hart appointed as standby counsel. Doc. 100.

On April 2, 2020, Mr. Bandy filed the instant motion to suppress. Doc. 53. In the motion, which he filed *pro se* without assistance from his standby counsel, he asks the Court to determine

whether there was sufficient probable cause to justify the search of his residence, and whether the use of IP information rendered the issuance of the search warrant improper. *See generally* Doc. 53. Mr. Bandy does not cite any legal authority, but because the motion is *pro se*, it is appropriate that it be “liberally construed” even if “inartfully pleaded.” *Estelle v. Gamble*, 429 U.S. 97, 106 (1976). The Government responds that there was probable cause to support authorization of the search warrant. Doc. 54 at 13. Further, the Government argues that a variety of evidentiary facts were used in the application for a search warrant, not just IP information, and regardless, a number of courts have already held that probable cause can be successfully established through the use of an IP address. *Id.* at 14–15.

## DISCUSSION

The Court has now reviewed the parties’ briefs and the relevant Fourth Amendment law. For the reasons explained below, it finds that the totality of the circumstances gave Magistrate Judge Laura Fashing probable cause to believe that evidence and instrumentalities of the crime were located at Mr. Bandy’s residence. As a result, the search did not violate Mr. Bandy’s Fourth Amendment rights and the evidence discovered will not be suppressed. The Court also finds that the use of IP information did not render the search warrant improper, as IP addresses are sufficient to establish probable cause.

### **I. Whether Sufficient Probable Cause Existed to Justify the Search of Mr. Bandy’s Residence**

On the merits, Mr. Bandy argues that the Government failed to identify his cable router and show that it was located at his residence in his possession, and that accordingly there were insufficient grounds to justify the search. Doc. 53 at 5. He states that the Government’s search warrant was based on a letter from Comcast that oversimplifies IP addresses and is “insufficient, deceptive, and misleading.” *Id.* at 1. As the Tenth Circuit has explained, probable cause to issue

a search warrant exists when the facts and circumstances laid out in the supporting affidavit “would lead a prudent person to believe a fair probability exists that contraband or evidence of a crime will be found in a particular place.” *United States v. Basham*, 268 F.3d 1199, 1203 (10th Cir. 2001) (internal citations omitted). The task of an issuing judge is “to make a practical, common-sense determination” from the totality of the circumstances whether “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). The issuing judge is expected to draw reasonable inferences from information found in the affidavits. *See United States v. Rowland*, 145 F.3d 1194, 1205 (10th Cir.1998). Probable cause is more than a mere suspicion, but considerably less than what is necessary to convict someone. *United States v. Ventresca*, 380 U.S. 102 (1965).

Mr. Bandy argues that the Government was required to present information regarding the unique cable router address belonging to the router supplied to him by Comcast in order to obtain a search warrant. Doc. 53 at 5. He states that there were insufficient grounds to justify the search of his residence because the Government failed to address certain technical matters in its affidavit. *Id.* Mr. Bandy asserts the Government did not present evidence that his cable router was configured by Comcast, or address whether the router was public and accessible to all 12.5 million Comcast customers. *Id.* at 2. He argues that Comcast’s subscribers are not assigned a single, constant IP address, but rather are given a dynamic IP address that can potentially change several times. *Id.* Mr. Bandy then asserts that Comcast’s system of allocating IP addresses uses Dynamic Host Configuration Protocol (DHCP), which makes it impossible for Comcast to assign an IP address to a human being or piece of property. *Id.* at 3. Mr. Bandy next argues that an IP address is dependent on the hardware Media Access Control (MAC) address of the network interface on the cable router. *Id.* at 4. He notes that most cable routers have three hardware MAC addresses

assigned and that cable routers can be easily moved. *Id.* Mr. Bandy states that the Government, in obtaining the search warrant using the IP address identified by Comcast, did not “demonstrate knowledge of the required MAC address, or take steps to verify that the cable router ... was present on the property in Chris Bandy’s possession.” *Id.*

However, there is no requirement that specific information regarding an individual’s MAC address or cable router must be presented in order to establish probable cause. *See Basham*, 268 F.3d at 1203. Rather, the requirement for probable cause to issue a search warrant is that under the totality of circumstances, the supporting affidavit must lay out facts and circumstances establishing a fair probability that contraband or evidence of a crime will be found in a particular place. *Id.* The totality of circumstances evaluation of probable cause may include the factor of ownership and control of a residence and its possession by a person, and a determination of probable cause does not mean that law enforcement agents will know the exact form of evidence that will be present at the location to be searched. *See United States v. Horn*, 187 F.3d 781, 787–88 (8th Cir. 1999); *United States v. Reyes*, 798 F.2d 380, 383 (10th Cir. 1986)). Here, the supporting affidavit described in great detail with evidentiary facts from the investigation that Mr. Bandy had been identified as the author of the criminal electronic communications. Doc. 54 at 14. The evidentiary facts included confirmation of Mr. Bandy’s physical address; the IP address used in sending the harassing electronic communications, which was also used in Mr. Bandy’s banking profile; his work history with the victim and their shared workplace; the repetitive themes of the sexually charged emails; and his motive for retribution against M.D. for overseeing his termination. *Id.* at 14–15. The affidavit detailed the investigation’s steps, described with specificity the property-residence to be searched (with reference photographs), and described with specificity the particularized items to be seized. *Id.* The items to be seized included computers or

storage media that could be used as a means to violate 18 U.S.C. § 2261A; evidence of who used the computer or storage medium; evidence of how and when the computer was accessed; passwords, encryption keys, and other devices necessary to access the computer; records of the computer's internet history; routers, modems, and network equipment used to connect computers to the internet; and records and information related to various account names that were used to send the harassing communications described in the affidavit. Doc. 54-2 at 14–16. The FBI special agent corroborated the evidentiary facts before presenting the search warrant application to the U.S. Magistrate. *Id.*

Additionally, the Government's application for a search warrant was not rendered invalid, as Mr. Bandy alleges, by a failure to prove that a specific router was in Mr. Bandy's home. The actual presence of a particular router at Mr. Bandy's residence does not impact the likelihood that such a device would be found there, and it was reasonable based on the search warrant application for Magistrate Judge Laura Fashing to conclude that the router supplied by Comcast to Mr. Bandy for home internet service would be located at his residence. *Id.* at 13 n.2; 15.

Here, the search warrant was granted on the basis of numerous factors that linked the offensive emails to Mr. Bandy, including information that IP address 71.228.120.223 was registered to Mr. Bandy both before and after harassing emails were sent to the victim, M.D. and that a person with access to Mr. Bandy's personal banking account used the same IP address. Doc. 54 at 13. The search warrant application was compiled using reports on the investigation, results of physical and electronic surveillance conducted by law enforcement agents, investigation and analysis by FBI agents and computer forensic professionals, and information from administrative subpoenas. *See* Search Warrant Application, Doc. 54-2 at 2. Further, the search warrant application identified how agents traced the emails to Mr. Bandy using his IP address; how Mr.

Bandy allegedly used virtual private servers to attempt to mask his identity; and how he allegedly created multiple accounts and used multiple forms of communications to send messages and hide his identity. Doc. 54-2 at 4–6. The application also included pictures of Mr. Bandy’s residence and stated with particularity the items to be seized.

The Court finds that, under the totality of the circumstances, Magistrate Judge Laura Fashing had probable cause to believe that evidence and instrumentalities of the crime were located at Mr. Bandy’s residence. The application and affidavit are detailed in explaining the investigation of the instant offense and create a fair probability that a search of Mr. Bandy’s residence would produce evidence. Mr. Bandy’s assertion that there were insufficient grounds to justify the search, and that it was a “fishing expedition” does not pass muster in light of the Tenth Circuit’s caselaw. The Government was not required to produce the hardware cable router address or prove that it was at Mr. Bandy’s residence at the time of the search. Given that the application and affidavit thoroughly alleged a fair probability exists that evidence of the electronic communications involved in this crime would be found at Mr. Bandy’s residence, there was sufficient grounds to justify the search.

## **II. Whether the Use of IP Address Information Renders the Search and Seizure Unlawful**

Mr. Bandy argues that the Government’s application for a search warrant failed to address the matter of who had access to his cable router and misleadingly represented that an IP address is adequate to identify an individual. Doc. 53 at 5. He attaches two exhibits to support his claim that using an IP address to obtain and carry out a search warrant is misleading and deceptive. Doc. 53, Exs. 1 and 2. He argues that these exhibits prove that using IP address information “harm[s] innocent people’s lives.” Doc. 53 at 4–5.<sup>1</sup> Mr. Bandy’s arguments and exhibits demonstrate that

---

<sup>1</sup> Exhibit 1 is an article by the Electronic Frontier Foundation titled “Unreliable Informants: IP Addresses,

there are certainly challenges associated with using IP addresses to investigate online crimes, but ultimately the analysis of Fourth Amendment probable cause is unchanged. For the reasons explained below, the Court finds that the use of Mr. Bandy's IP address did not violate the Fourth Amendment as it has been interpreted in the caselaw.

Appellate courts, including the Tenth Circuit, have consistently found that there is probable cause where affidavits explain how, with thorough investigation, online crimes have been tracked to a defendant's IP address and his home. *See, e.g., United States v. Renigar*, 613 F.3d 990, 994 (10th Cir. 2010) (holding affidavit that explained child pornography was being shared from specific IP address provided sufficient probable cause to search residence associated with IP address); *United States v. Chiaradio*, 684 F.3d 265, 279 (5th Cir. 2012) (finding probable cause where affidavit explained how investigation led to defendant's IP address and, in turn, his home); *United States v. Vosburgh*, 602 F.3d 512, 526 (3rd Cir. 2010) (finding it was "fairly probable" child pornography may be located on computer equipment found in defendant's home where affidavit provided that someone using a computer with IP address used to download child pornography was assigned to the internet account registered to defendant's home); *Perez*, 484 F.3d at 740 (finding "an association between an IP address and a physical address" is a substantial basis to conclude that evidence of criminal activity may be afoot inside an individual's residence).

Mr. Bandy argues that it is a Fourth Amendment violation "to search an individual's home based on bare assertions that some crime was committed using an IP address associated with a location or a person." Doc. 53 at 3 (citing Ex. 1 at 14). He asserts that any of Comcast's 12.5

---

Digital Tips and Police Raids." It explains the limitations of IP Addresses and how they *alone* cannot reliably locate or identify a suspect. Doc. 53, Ex. 1 at 4. Exhibit 2 is a Law Review student Note that argues IP addresses are inherently unreliable and should be corroborated and used with caution in obtaining search warrants. Erin Larson, *Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?*, 18 N.C. J.L. & Tech. 316 (2017).

million internet customers could have accessed his cable router from any public area nearby, such as his “front yard, street, neighbor’s yards and houses, [or via] cell phones.” *Id.* at 2. Mr. Bandy argues that police are required to address whether an internet subscriber has an open wireless connection before they have probable cause to believe that an individual associated with an IP address is the suspect. Doc. 53 Ex. 1 at 17–18. However, Mr. Bandy’s citation for this proposition does not state that law enforcement officers have a requirement to take such steps before probable cause is established. *Id.* Rather, the Electronic Frontier Foundation article recommends best practices for using IP address information in criminal investigations, and it indicates that additional inquiries be conducted to verify and corroborate physical locations and whether multiple people are using an IP address. *Id.* at 18. Here, that is precisely what the investigators did: they verified Mr. Bandy’s physical address and observed him at his residence to determine whether the IP address was associated with “a café, library, business, organization, multi-room apartment, or house shared by several people.” Doc. 53 Ex. 1 at 17. There is no indication that the agents failed to verify Mr. Bandy’s address and other information in obtaining the search warrant. This article’s recommendations are valuable; in particular, the urge for police and judges to be more ambitious in corroborating IP address information. However, in Mr. Bandy’s case, law enforcement *did* employ the best practices for using an IP address in a criminal investigation.

Mr. Bandy’s second exhibit, a student note from the North Carolina Journal of Law & Technology, has similarly useful recommendations but does not change the outcome of his motion. Doc. 53 Ex. 2. The author argues that “IP addresses alone should not provide sufficient probable cause to obtain a search warrant and that more substantive information should be required to issue a warrant.” Larson, *Tracking Criminals with Internet Protocol Addresses*, 18 N.C. J.L. & Tech. at 320–21. But here, law enforcement outlined numerous evidentiary facts in the search warrant

application, going far beyond simple use of only an IP address. Doc. 54 at 14–15. The application includes confirmation of Mr. Bandy’s physical address, his work history with the victim and their shared workplace, the repetitive themes of the sexually charged emails, and his motive for retribution against M.D. for overseeing his termination. *Id.* Although Mr. Bandy repeatedly argues that it is a Fourth Amendment violation “to search an individual’s home based on bare assertions that some crime was committed using an IP address associated with a location or a person,” Doc. 53 at 3 (citing Ex. 1 at 14), this case does not involve “bare assertions.” The application for the search warrant provides a variety of evidentiary facts regarding the thorough investigation to link Mr. Bandy to the offense, including confirmation of Mr. Bandy’s physical address, the IP address used to send the harassing electronic communications and used to access Mr. Bandy’s banking profile, his work history with the victim and their shared workplace, the repetitive themes of the sexually charged emails, and his motive for retribution against M.D. for overseeing his termination. Doc. 54-2; Doc. 54 at 14–15. Further, these facts were corroborated by the FBI special agent before the application was presented to the magistrate judge. *Id.*


The caselaw of the Tenth Circuit confirms that when information in an affidavit would cause a person of reasonable caution to believe that evidence of an electronic crime will be found at the residential address in question, there is sufficient probable cause. *See Renigar*, 613 F.3d at 994; *United States v. Adams*, No. CR 18-3413 KG, 2019 WL 6784073, at \*4 (D.N.M. Dec. 12, 2019) (unreported). The Tenth Circuit has held that when information links the IP address in question to both evidence of a crime and to a residential address, there is a strong suggestion that the computer which accesses the network will be found at the residence and will contain evidence associated with the crime. *Renigar*, 613 F.3d at 994. Accordingly, under the caselaw of the Tenth Circuit and in accordance with the best practices outlined in Mr. Bandy’s exhibits, the use of IP

address information in this case was sufficient and proper to find probable cause to search his residence.

### CONCLUSION

For the reasons set forth above, the Court finds that the search warrant application thoroughly alleged a fair probability that evidence of the electronic communications involved in this crime would be found at Mr. Bandy's residence. The Court also finds that great scrutiny was employed regarding the use of IP address information and that there was sufficient evidence used in the application for a search warrant. Law enforcement had probable cause to justify the search and the use of Mr. Bandy's IP address did not render the search and seizure unlawful. Therefore, law enforcement did not violate Mr. Bandy's Fourth Amendment rights and the physical evidence they discovered will not be suppressed.<sup>2</sup> Mr. Bandy's Motion to Suppress Evidence [Doc. 53] is accordingly **DENIED**.

Dated this 5th day of February, 2021.

  
\_\_\_\_\_  
MARTHA VÁZQUEZ  
UNITED STATES DISTRICT JUDGE

---

<sup>2</sup> The Government also filed a supplement to its response involving a recorded and transcribed jail call that Mr. Bandy made on March 9, 2020 to his sister. Doc. 80. The Court finds that it is unnecessary to address this information in order to resolve the motion to suppress.